FEDERAL PUBLIC KEY INFRASTRUCTURE (FPKI) ANNUAL REVIEW REQUIREMENTS

Version v1.0

April 11, 2017

Abstract

This document supersedes the Federal PKI Compliance Audit Review Requirements document and provides an overview of the annual review submission required to remain in good standing with the Federal PKI.

REVISION HISTORY TABLE

04/11/2017	1.0	Final Release	FPKI Support Team

Table of Contents

1. Introduction

This document provides detailed guidance to participating Public Key Infrastructures (PKIs) and their auditors for meeting the annual review requirements of the Federal PKI (FPKI). Each year, the FPKI reviews its relationship with each cross-certified or subordinated organization to ensure the continuing integrity of the trust environment. The review requires the submission of documentation and artifacts by the FPKI members.

This document provides:

- Guidance regarding the performance and reporting of annual compliance audits, and
- Instructions for PKI Owners/Operators regarding submission of Annual Review Packages.

1.1. Scope

All organizations operating a PKI that is cross-certified with the Federal PKI, whether via the Federal Bridge Certification Authority (FBCA) or directly with the Federal Common Policy (COMMON) Root Certification Authority (CA), or subordinated under the COMMON Root CA must submit an Annual Review Package to the Federal PKI Policy Authority (FPKIPA).

1.2. Audience/Responsibilities

This document pertains to PKI Owners/Operators wishing to maintain their relationship with the FPKI and the independent third-party auditors that conduct the Annual Audit Assessments.

- PKI Owners/Operators are responsible for the ongoing conformance of their PKIs (see Appendix A) and submission of the completed Annual Review Package.
- Third-Party Auditors are responsible for the detailed review of the PKI CP, CPS, Memorandum of Agreement (MOA), as well as other relevant documents such as Key Recovery Policy (KRP), Key Recovery Practice Statement (KRPS), detailed review of operations and operational environment, and for issuing an opinion concerning the compliance of the operations of the PKI with its CP.

1.2.1. PKI Owner/Operator Responsibilities

The organization operating the CA is considered the PKI Owner/Operator and has the responsibility to:

- Ensure audits have been completed for the entirety of the PKI within the scope of its CP; components/functions that are separately managed and operated must be included.
- Clearly identify each PIV and/or PIV-I card configuration in its PKI and ensure that each configuration has undergone annual card testing and all identified issues have been addressed/remediated.
- Gather and submit end-entity production certificates to the FPKIPA for testing.
- Assemble and submit the Annual Review Package to the FPKIPA.

1.2.2. Auditor Responsibilities

The auditor of a CA shall evaluate the applicable CPS in regard to the governing CP and render an opinion concerning conformance of the CPS.

The auditor(s) shall examine PKI operations in regard to the CPS, RAA, MOA, and other relevant documentation and render an opinion as to whether the operations implement the requirements of these documents.

1.3. Package Submission

The Annual Review Package must be submitted in accordance with the FPKI review schedule to: icam@gsa.gov. Sensitive information may be submitted directly to the Chair, FPKIPA.

The CP or CPS must be submitted in MS-Word format.

Note: The FPKI Annual Review Schedule may be found at www.idmanagement.gov.

1.4. Background - Annual Review Package

The Annual Review Package is the responsibility of the PKI Owner/Operator. It must be submitted to the FPKIPA on an annual basis and shall contain the following, when applicable:

- Assertion of Scope – An authorized representative of the PKI shall assert that the Annual Review Package includes a complete audit of the entire PKI and encompasses all components of the PKI including any that may be separately managed and operated. (See Section 5.1)
- Architectural Overview - A detailed description of the components of the PKI and their relationship. Include a diagram of the infrastructure with enough detail to show the individual components of the PKI and the physical/logical security associated with them, including any components operated by a third party. Provide the number of active certificates associated with each CA and identify known relying parties. (See Section 5.2)
- Independent Third-Party Audit Opinion Letter(s) (also called Audit Letters) – One or more letters signed by the auditor(s) that encompass the entirety of the PKI being assessed. (See Section 5.3)
- Auditor Documentation Review and Assertion – Statement from the auditor that annual PIV card test reports (if applicable), certificate test results, Registration Authority Agreements (RAA), where applicable, and memoranda of agreement are on file. (See Section 5.3)
- Audit Findings and Plan of Actions and Milestones – In the event there are findings associated with the audit, the PKI owner/operator shall prepare a detailed report of the findings and a detailed remediation plan with dates and milestones on how findings will be remediated. (See Section 5.4)
- PIV and PIV-I Test Reports – The test reports from each sample PIV and or PIV-I production card for each configuration administered by the PKI Owner/Operator showing they successfully passed the GSA FIPS 201 Evaluation Program annual card testing. (See Section 5.5)

- Certificate Artifacts for Interoperability Testing – A detailed description of the CAs in the participating organization's PKI and the types of certificates issued by each that utilize certificate policy object identifiers (OIDs) for which a path exists to the FPKI. Submit example certificates that represent all of the identified certificate types. Note: where more than one issuing CA is in use, submit the full complement of certificate types issued by each issuing CA. (See Section 5.6)
- Current CP or CPS – A redlined CP (CPS for organizations subordinated under the Federal Common Policy CA) showing all changes made to the CP (CPS) since the last annual submission. (See Section 5.7)

2. Audit Requirements

Independent compliance audits are the primary mechanism used by FPKIPA to ensure participating PKIs are operating in conformance to the requirements identified in the associated Certificate Policy (CP).

The Certificate Policy (CP) establishes the requirements for operating and managing a PKI, to include the operations and management of the CA, Registration Authority (RA), Repositories, Credential Status Services (CSS), and related security-relevant ancillary components (e.g. Card Management System (CMS)). The Certification Practice Statement (CPS) describes how the CP requirements are met by the operational system.

2.1. FPKI Shared Service Providers

FPKI Shared Service Providers (SSPs) are PKI Owner/Operators required to operate in compliance with the COMMON CP. Their CPSs must describe how the requirements of the COMMON CP are met and their operations must implement those requirements.

The FPKI SSP operates a Certification Authority (CA) that issues and revokes digital certificates for PIV Cards, maintains the certificate repository and issues Certificate Revocation Lists (CRL); while the issuing federal agency is responsible for the identity proofing, enrollment, certificate request, and card issuance activities associated with the PIV program, collectively referred to as Registration activities. The FPKI SSP must execute a formal Registration Authority Agreement (RAA) with any organization, including the federal agency customer, that provides identity proofing, enrollment, certificate request and/or card issuance activities.[1]

The Annual Review Package must contain audit letters covering all aspects of the PIV Credential Issuance program.

Federal agency implementation of a PIV issuance system is subject to two additional assessments:

- NIST Special Publication 800-79 Assessments
- FISMA Review/ATO/POA&M

[1] The *FPKI Shared Service Provider Roadmap* introduced the requirement for a Registration Practices Statement between SSPs and customer agencies. The *FPKI Registration Authority Agreement Template and Guidance* document provides specific guidance on the development of such a document.

While similar in scope to the annual audit, neither is a substitute for the annual independent Third-party audit opinion letter.

2.2. Cross-Certified PKIs

PKI Owner/Operators cross-certified with the FPKI maintain their own certificate policies, certification practice statements and operational environments. The trust relationship with the Federal PKI is based on a comprehensive comparability mapping of the cross-certified organization's CP to the FBCA CP.

The Annual Review Package must contain audit letters covering all aspects of the cross-certified organization's PKI.

In addition, those providing PIV-I cards on behalf of Federal agencies must meet all of the requirements of the customer agency's Authority to Operate.

2.3. Bridges

A Bridge PKI Owner/Operator must submit an Annual Review Package that covers all aspects of the Bridge's operations. The FPKI reserves the right to request additional documentation to determine if the Bridge's processes remain comparable or equivalent to FPKI processes.

In addition, the Bridge PKI Owner/Operator is responsible for ensuring that its member PKIs are fully audited in accordance with the agreed upon audit standards.

The Bridge's auditor is responsible for verifying member PKI audits are on file and current.

3. Auditor Qualifications

The FPKIPA reserves the right to review the qualifications and experience of any auditor whose opinion letter is submitted as part of an Annual Review Package. In order to be qualified, an auditor must:

- Perform audits as a regular ongoing business activity.
- Demonstrate competence in the field of PKI compliance audits – there must be a history of performing PKI compliance audits that spans several years.
- Be thoroughly familiar with the requirements of the CP associated with the audit performed.
- Provide attestations of independence from the audited organization.

4. Annual PKI Compliance Audit Requirements

The audit includes two primary components:

- Review of the CPS resulting in an opinion concerning whether the CPS adequately addresses all the requirements of the CP.
- Review of the operations of the PKI against the CPS resulting in an opinion as to whether the operations and management of the PKI correctly implement the CPS.

4.1. Audit Methodology

The FPKI does not specify the audit methodology to be used; however, if a specific methodology is used, it must be identified in the audit opinion letter.

4.1.1. Documentation Review

Regardless of the audit methodology used, the following documentation shall be included in the review:

- Current CP and CPS: The auditor shall verify that the CPS implements the requirements of the CP in a satisfactory manner.
- Current KRP and KRPS: Where applicable, the auditor shall verify that the KRPS implements the requirements of the KRP in a satisfactory manner. (Note: KRP/KRPS requirements may be integrated with the CP/CPS and audited as part of those documents.)
- PIV/PIV-I Test Reports: For PIV and PIV-I Issuers, a sample production card for each configuration issued must successfully pass the GSA FIPS 201 Evaluation Program annual card testing. The auditor shall obtain and document what test reports were provided as evidence that this testing was satisfactorily performed during the 12-month audit period.
- Current Memorandum of Agreement (MOA): The auditor shall verify a current MOA has been executed between the PKI Owner/Operator and the FPKIPA, and the PKI Owner/Operator is complying with all provisions and obligations detailed in the MOA. A statement to this effect should be included in the *Audit Opinion Letter*.
  Note: If the PKI Owner/Operator maintains MOA(s) with other organizations, these are also within the audit scope and must be reviewed for compliance.
- Certificate Test Results: The auditor shall obtain and document what test reports were provided as evidence that certificate testing was satisfactorily performed during the 12-month audit period.
- Current Registration Authority Agreement (RAA): Where applicable, the auditor shall verify an RAA has been executed between the PKI Owner/Operator and the organization performing RA services and said organization is complying with all provisions and obligations detailed in the RAA. A statement to this effect should be included in the *Audit Opinion Letter*.
  Note: In the event the RA services are audited separately and by a different auditor or group of auditors, these separate audit opinion letters must be included in the Annual Review Package.
- Last previous annual audit opinion and findings - All audits shall include a review of the results of the previous annual audit opinion and findings, and verification that the remediation of the findings was completed satisfactorily.

4.1.2. Use of Sampling

Sampling may be used as allowed by policy. If the auditor uses sampling, all PKI components, PKI component managers, and operators to which the sampling applies shall be considered in

the sample. All such samples will vary on an annual basis, such that the entire complement of components undergoes auditing within a timeframe to be established in the applicable MOA. Each year, previous sampling results will be reviewed, with an emphasis on determining whether discrepancies and deficiencies have been rectified.

4.2. Types of Audit

4.2.1. Full Operational Audit

PKI Owner/Operators cross-certified with the FBCA or subordinated under the COMMON Root CA will undergo a *Full Operational Audit* each year that includes evaluation of all operational practices encompassing the scope of the applicable CP and CPS. Included in this evaluation, the auditor shall review previous compliance audit findings for associated changes and corrective actions.

There are two exceptions to the Full Operational Audit that may be utilized depending on circumstances.

4.2.2. Day-Zero Audit

Note: Bridge PKI Owner/Operators are not permitted to utilize Day-Zero Audits.

PKI Owner/Operators may utilize a "Day-Zero audit" for a newly-established CA.

Newly established CAs have the policy, procedures, and resources to operate; however, they have not accumulated sufficient operational evidence for evaluation against the appropriate CP/CPS. The Day-Zero Audit concentrates on the policies and procedures associated with the newly established CA, and the limited operational data that may be available.

PKI Owner/Operators that choose to submit a Day-Zero Audit must complete a full operational audit, including a complete assessment of all operational practices, within one year of the Day-Zero Audit.

Note: Additional information regarding Day-Zero Audit Letter requirements may be found in Appendix B-2.

5. Annual Review Package

See Appendix C for a checklist of what constitutes a complete Annual Review Package.

On an annual basis, all PKI Owner/Operators operating a PKI that is cross-certified with the Federal PKI, whether via the Federal Bridge Certification Authority (FBCA) or directly with the Federal Common Policy (COMMON) Root CA, or subordinated under the COMMON Root CA must submit an Annual Review Package to the FPKIPA that contains the following:

5.1. Assertion of Audit Scope

This will take the form of a letter or memorandum on the letterhead of the PKI Owner/Operator's organization and shall:

- Assert that the Annual Review Package represents a complete audit of the entire PKI and encompasses all components of the PKI, including any that may be separately managed and operated.
- Identify the period covered by the audit and the dates the audit was conducted.
- Identify the current CP and CPS(s) by name and version number,
- Identify those functions that are separately managed and operated, along with the identity of the organization responsible for those functions.
- If multiple Audit Opinion Letters are included in the Annual Review Package, list these and indicate which components and functions are covered by each.

The letter shall be signed by an authorized representative the PKI.

5.2. Architectural Overview

As an attachment to the *Assertion of Audit Scope*, the PKI Owner/Operator shall include an architectural overview. At a minimum, this overview will include:

- A list of all the CAs associated with the PKI, including all subordinated CAs and other cross-certificate relationships.
- A list of the URLs for OCSP Responders and CRL Distribution Points included in certificates issued by the CA.
- For each identified CA, its purpose and any known federal government applications that accept these certificates.
- For Shared Service Providers, a list of supported organizations.
- A detailed description of the security-relevant components of the PKI (CA, CMS, CSS, RA), identifying those that are separately managed and operated.
- Diagrams showing the logical network view and logical architectural view of the infrastructure with enough detail to show the security-relevant components of the PKI and the physical/logical security associated with them. The diagram must depict those components that are separately managed and operated, and their connectivity to the CA.
- The number of certificates issued by each issuing CA during the review period, the total number of certificates supported at the time the package is prepared and submitted, and a list of known relying parties (list of organizations, programs, and points of contact).

5.3. Audit Opinion Letter(s)

The requirements of the Audit Opinion Letter(s) are detailed in Appendices B-1 and B-2.

The Annual Review Package will include one or more Audit Opinion Letters that together encompass the entirety of the PKI scope.

5.3.1. Web Trust for CA

The current Web Trust for CA audit methodology does not satisfy the requirements for ensuring the requirements of the CP are fully addressed. Therefore, when the Web Trust for CA audit

methodology is used, it must be accompanied by a signed Management Assertion from an authorized representative of the PKI Owner/Operator as follows:

- The CPS conforms to the requirements of the CP;
- The PKI is operated in conformance with the requirements of the CPS;
- The PKI has maintained effective controls to provide reasonable assurance that procedures defined in Section 1 – 9 of the Entity CPS are in place and operational;
- The PKI is operated in conformance with the requirements of all cross-certification MOAs executed by the organization.

The Management Assertion Letter must be appended to the Audit Opinion Letter; and the Audit Opinion Letter must state that management's assertions have been evaluated and provide an opinion as to whether they are fairly stated in relation to the PKI being audited.

5.3.2. Multiple Audit Opinion Letters

If multiple Audit Opinion Letters are submitted, each shall be signed by its respective auditor. The PKI Owner/Operator will clearly identify what CA(s) and/or PKI components and functions are covered by each letter in the *Assertion of Audit Scope* and will ensure that all PKI components and functions under the overall responsibility of the participating PKI PMA, including those that are separately managed and operated, are included in the package.

5.4. Audit Issues and Audit Plan of Actions and Milestones

The PKI Owner/Operator will include a description of any audit issues/findings, along with an Audit Plan of Actions and Milestones (POA&M) detailing the action taken or that will be taken to remediate the issues/findings along with the expected completion date.

5.5. PIV and PIV-I Test Results

For PKI Owner/Operators that issue PIV and PIV-I credentials, copies of the successfully completed PIV and/or PIV-I Test Report(s) that cover all distinct credential configurations must be included in the Annual Review Package.

5.6. Certificate Artifacts for Interoperability Testing

The Federal PKI conducts credential testing for all certificate types issued by a particular CA on an annual basis.

- The PKI Owner/Operator shall submit sample certificates sufficient to ensure at least one sample of every type of end-user certificate from each issuing CA for which a path to the FPKI exists via CA certificates issued to the organization's PKI from the FPKI. Types of certificate are indicated by the corresponding certificate usage (e.g. signature, encryption, authentication, etc.) and asserted policy.
- The submitted end-user certificates shall have been issued within the preceding twelve (12) months.
- The certificate file names will be sufficient to identify the type of certificate and its issuing CA.

- The certificates shall be operational and in use by the PKI Owner/Operator's users.

The FPKI will conduct credential testing and notify the PKI Owner/Operator of any discrepancies found. The PKI Owner/Operator is responsible for incorporating these findings into the Audit POA&M.

Note: CAs that remain operational for maintenance purposes, but have not issued any certificates during the preceding 12 months, should be identified as such and are exempt from submitting sample certificates.

5.7. Current CP or CPS

The PKI Owner/Operator shall submit a redlined version of its current CP (CPS for FPKI SSPs subordinated under the Federal Common Policy CA) showing all changes made to the CP (CPS) since the last annual submission. All applicable ratified FPKI CP (FBCA or COMMON) change proposals must have been incorporated into the organization's CP.

Appendix A FPKI Member Continuous Maintenance Requirements

This Appendix provides guidance for the day-to-day maintenance of the PKI Owner/Operator's relationship with the FPKI. It is provided as a quick guide to ensuring the continuing health of the FPKI trust community.

Ongoing actions and controls

PKI Owners/Operators must implement the following controls on a continuous basis and provide supporting documentation to the FPKI annually (see *FPKI Annual Review Requirements*), in order to ensure that they meet agreed-upon levels of conformance and trust:

- **Policy Conformance** controls that ensure that Affiliate CP remains aligned with the Federal PKI Policy
- **Technical Architecture** controls to ensure technical interoperability between the Affiliate and the Federal FPKI
- **Testing** controls to ensure that issued certificates and PIV/PIV-I Cards are secure and conformant
- **Governance** controls to ensure that all MOAs are kept current
- **Audit** selection and scheduling controls to ensure that compliance audits are performed annually
- **Participation in the Certificate Policy Working Group and FPKI Policy Authority** to stay abreast of ongoing issues and priorities

Control Area	Required Actions & Controls
Policy Conformance	– The FPKIPA updates the FPKI COMMON CP or FBCA CP using the Change Proposal process. 1. Organizations cross-certified with a FPKI CA must ensure their CPs continue to align with the appropriate FPKI CP, as necessary. 2. Organizations subordinated to the Federal Common Policy CA must ensure their CPSs continue to comply with the Common CP. 3. Bridges and PKI Service Providers must ensure their members/customers stay aligned, as appropriate. – The FPKI reviews policy conformance during the Annual Review.
Technical Architecture	– Updates made to a FPKI member organization's technical architecture must be reported to the FPKIPA at the time the change is implemented. Examples of reportable updates include but are not limited to: • Addition of new Certification Authorities • Changes to PKI repositories that introduce or eliminate support for different protocols • Changes to PIV/PIV-I Issuers that would affect their certificates and/or cards – Impacts on security posture or interoperability are assessed by the FPKIPA. Failure to resolve issues identified by the

Control Area	Required Actions & Controls
	FPKIPA may result in termination of the MOA/cross-certificate. – The FPKI reviews current architecture during its Annual Review even if no changes have been reported.
Testing	– Organizations must conform to the applicable Federal PKI certificate profiles. – Organizations shall submit sample production certificates to the FPKIPA for testing during the Annual Review. The submission must include a sample certificate for each certificate type issued by the CAs under the cross-certified organization's purview (e.g. identity, signature, encryption, code signing etc.). – The FPKI reviews the credentials for conformance to the certificate profiles (as appropriate) and relevant PKIX guidance. – For Organizations that issue PIV/PIV-I cards, each PIV/PIV-I Card Configuration shall be scheduled for testing by the FIPS 201 Evaluation Program and completed successfully prior to completion of the Annual Review. This testing requires in-person attendance by the holder of the PIV/PIV-I card.
Governance	– Organizations must ensure a valid MOA has been executed between the organization and the FPKI. MOAs are valid for up to three years, and must be renewed whenever new cross-certificates are issued. – FPKI Shared Service Providers that issue PIV certificates on behalf of Federal organizations must abide by the *GSA IT Security Procedural Guide: Managing Enterprise Risk Security Assessment and Authorization, Planning, and Risk Assessment CIO-IT Security – 06-30* and maintain a valid Authority to Operate through the GSA FISMA Assessment process. – Organizations that issue PIV-I cards on behalf of Federal agencies must meet all of the requirements of the customer agency's FISMA Assessment process and maintain a valid Authority to Operate. – Bridges must establish and maintain processes for governance and oversight of their cross-certified members. – The FPKI reviews governance documentation during the Annual Review process.
Audit	– FPKI member organizations shall have annual third-party audits conducted on their PKIs in accordance with the requirements published in the *FPKI Annual Review Requirements* document and submit these audits for review according to the schedule published by the FPKIPA. – The FPKI reserves the right to request that an organization conduct an out-of-cycle compliance audit on any of its CAs.

Control Area	Required Actions & Controls
	– The FPKI reserves the right to request additional detail related to the audits of member organization CAs or Bridge Member CAs. – The FPKI reviews audit documentation during the Annual Review process.

Plan of Action and Milestones

FPKI member organizations shall submit a Plan of Actions and Milestones (POA&M) during the Annual Review that describes all identified issues, the proposed resolution for each, and the status of each.

If security issues are identified at any point during the Annual Review process and cannot be resolved, the FPKIPA may revoke the Organization's cross-certificate.

Appendix B-1 Audit Opinion Letter Checklist

All audit opinion letters will include the following:

Category	Requirement	Description
General	**Signature**	The Audit Opinion Letter shall be addressed to the participating PKI PMA and shall be signed by the auditor. **NOTE:** *The signature may be the corporate signature of the audit firm or the signature of the head of the independent office within the participating PKI organization (e.g., the organization's Inspector General)*
Auditor Background Information	**Identity**	Identity of the Auditor(s) and the individuals performing the audit.
	Competence	Competence of the Auditor(s) to perform compliance audits as required by the applicable CP and CPS.
	Experience	Experience of the individuals performing the audit in auditing PKI systems as required by the applicable CP and CPS.
	Objectivity	Relationship of the Auditor(s) to the participating PKI and the organization operating the component(s) being audited. This relationship must clearly demonstrate the independence of the Auditor(s) as required by the applicable CP and CPS.
Audit Scope	**Date Performed**	The date the audit was performed.
	Period of Performance	The period of performance the audit covers.
	Audit Methodology	Whether a particular methodology was used, and if so, what methodology. Note – if a "Web Trust for CA" audit methodology was used, a statement regarding management assertions must also be included.
	PKI Components in Scope	Which entity PKI component(s) were audited (CAs, CSSs, CMSs, and RAs).
	Documents Reviewed	Which documents were reviewed as a part of the audit, including document dates and version numbers. If portions of the PKI Policy are documented separately from the CP (e.g. a separate Key Recovery Policy & Practice Statement) these documents must also be reviewed as part of the audit.
Audit Results	**Statements concerning the Audit**	A statement that the operations of the audited component(s) were evaluated for conformance to the requirements of its CPS.
		A statement that CPS was evaluated for conformance to the associated CP.
		If applicable (always applicable for the cross-certified PKI's Principal CA), a statement that the operations of the component(s) were evaluated for conformance to the requirements of all cross-certification Memorandum of Agreement (MOAs) executed by the participating PKI with other entities.

Category	Requirement	Description
	Findings	Report any and all findings related to the evaluation of the operational conformance of the audited component(s) to the applicable CPS(s).
		Report any and all findings related to the evaluation of the CPS for conformance to the associated CP.
		If applicable (always applicable for the cross-certified PKI's Principal CA), report any and all findings related to the evaluation of the component(s) conformance to the requirements of all cross-certification MOAs executed by the participating PKI.
		Report whether sufficient documentary evidence was obtained, reviewed, and included with the audit package for: • Delta Mapping • Annual Certificate Testing • FIPS 201 Evaluation Program annual PIV/PIV-I Card Testing • Current MOA
	Closure of Previous Audit Cycle Findings	If applicable (always applicable if there were any findings reported the previous year), state that any findings from the previous audit were reviewed for closure.
	Summary of Changes	If applicable (most likely applicable if there were any change proposals to the corresponding FPKI CP (FBCA or COMMON)), state whether a summary of changes from the previous year was provided.
	Opinion	Provide an audit opinion concerning the sufficiency of the PKI operations in relation to the corresponding CP and CPS.

Appendix B-2 Special Considerations for Day-Zero Audit

Where a participating PKI component being audited is new, some procedures have only been performed in test environments or there is insufficient operational evidence to conduct a complete audit, the audit letter must include the following:

Category	Requirement	Description
General	**Signature**	The Audit Opinion Letter shall be addressed to the participating PKI PMA and shall be signed by the auditor. **NOTE:** *The signature may be the corporate signature of the audit firm or the signature of the head of the independent office within the participating PKI organization (e.g., the organization's Inspector General).*
Auditor Background Information	**Identity**	Identity of the Auditor(s) and the individuals performing the audit.
	Competence	Competence of the Auditor(s) to perform compliance audits as required by the applicable CP and CPS.
	Experience	Experience of the individuals performing the audit in auditing PKI systems as required by the applicable CP and CPS.
	Objectivity	Relationship of the Auditor(s) to the participating PKI and the organization operating the component(s) being audited. This relationship must clearly demonstrate the independence of the Auditor(s) as required by the applicable CP and CPS.
Audit Scope	**Date Performed**	The date the audit was performed.
	Period of Performance	The period of performance the audit covers.
	Audit Methodology	Whether a particular methodology was used, and if so, what methodology.
	PKI Components in Scope	Which entity PKI component(s) were audited (CAs, CSSs, CMSs, and RAs).
	Documents Reviewed	Which documents were reviewed as a part of the audit, including document dates and version numbers. If portions of the PKI Policy are documented separately from the CP (e.g. a separate Key Recovery Policy & Practice Statement) these documents must also be reviewed as part of the audit.
Audit Results	**Statements concerning the Audit**	A statement identifying which aspects of the PKI operations could be fully evaluated for conformance to the requirements of the PKI CPS.
		A statement that CPS was evaluated for conformance to the associated CP.
		A statement describing which procedures have not been performed on the operational system, but were evaluated for conformance to the requirements of the PKI CPS, but only with respect to training and written procedures.

Category	Requirement	Description
	Findings	Report any and all findings related to the evaluation of the operational conformance of the audited component(s) to the applicable CPS(s).
		Report any and all findings related to the evaluation of the CPS for conformance to the associated CP.
		If applicable (always applicable for the cross-certified PKI's Principal CA), report any and all findings related to the evaluation of the component(s) conformance to the requirements of all cross-certification MOAs executed by the participating PKI.
	Opinion	Provide an audit opinion concerning the sufficiency of the Day Zero PKI operations in relation to the corresponding CP and CPS.

Appendix C – Annual Review Package Checklist

This section provides additional guidance, questions, and comments that will assist in determining whether Annual Review Packages, including Auditor Letters of Compliance, are complete. Note that final determination is the responsibility of the FPKIPA.

Guidance	Commentary
Assertion of Audit Scope For PKIs with multiple components, state whether evidence of audit reports for all components has been provided.	Did the PKI Owner/Operator provide a cover letter and were all required Audit Opinion Letters and Auditor Compliance Summaries provided for all PKI components? Note: for a Bridge, is it clear what organization is responsible for the operations of each CA? And does the Bridge operate any issuing CAs?
Architectural Overview The architectural diagram should provide enough detail to show the security relevant components and identify the components that are separated managed and operated.	Did the PKI Owner/Operator provide an Architectural Overview and was there an accompanying diagram showing sufficient detail to assess the security posture of the PKI.
Current CP or CPS Cross certified entities must submit the current CP. Organizations subordinated under COMMON must submit the current CPS	Is this the CP/CPS identified by the auditor in the current audit report? Is there an auditor assertion that the CPS implements the CP?
Audit Date The date(s) the audit was performed.	Did each Audit Opinion Letter indicate the dates when the audits were performed? As a reality check, if the audit is performed in May of 2009, the date on the CP and CPS should not be July of 2009.
Audit Review Period State the dates covered by the audit.	Did each Audit Opinion Letter indicate the dates covered by the audit? As a reality check, if the audit is performed in May of 2009, the date covered should include the previous 12 months. This period may be shorter than 12 months if the PKI is newly established or may be slightly longer if there was a delay in scheduling the audit. However, there should not be a gap between the previous audit letter for the same components and this one; i.e. the current audit period start date should be continuous from the previous audit period end date.
Audit Methodology Whether a particular methodology was used, and if so, what methodology.	Did each Audit Opinion Letter indicate if a particular audit methodology was used, and if so, what methodology? The FPKI is methodology neutral.

Guidance	Commentary
Auditor Identity Identity of the Auditor and the individuals performing the audits.	Did each Audit Opinion Letter identify the auditor and the individuals performing the audit? Many of the big auditing concerns are partnerships or corporations that assert that the corporate entity performed the audit. While that's true in one sense, the FPKIPA wants the individual auditors identified – see the following regarding competence and experience.
Auditor Experience The auditor must be a Certified Information System Auditor (CISA) or IT security specialist, and a PKI subject matter specialist [see also FPKI and Common Policy CP Section 8.2].	Did each Audit Opinion Letter provide sufficient information for the FPKIPA to determine the competence and experience of the auditor? Individuals have competence, partnerships and corporations do not. The FPKIPA is looking for the individual auditor's credentials here. It's not enough to be a good auditor, the auditor should have some relevant IT or IT Security experience – or have audited a number of CAs.
Auditor Independence Relationship of the Auditor to the owner/operator of the PKI being audited. This relationship must clearly demonstrate the independence of the auditor from the entity operating or managing the PKI.	Did each Audit Opinion Letter provide sufficient information for the FPKIPA to determine the relationship and independence of the auditor to the PKI Owner/Operator that was audited? The Auditor needs to be independent and not conflicted. If there were multiple auditors auditing different components, each auditor must be independent both of the PKI Owner/Operator and of the organization operating the components being audited.
Audit Documentation Scope Which documents were reviewed as a part of the audit, including document dates and version numbers.	Did each Audit Opinion Letter provide a full list of relevant documents (i.e., CP, CPS, MOA) that were reviewed for each audited component, including dates and version numbers? At a MINIMUM the CP and CPS should be identified here – as well as any other documents relied upon in conducting the audit.
Audit Documentation Findings State that the CPS for the Principal CA and any other CPSs used by the PKI Owner/Operator were evaluated for conformance to the applicable CP. Report the findings of the evaluation of the CPS's conformance to the CP.	Did each Audit Opinion Letter state that the applicable CPS(s) were evaluated for conformance to the entity PKI's CP? Did each Audit Opinion Letter state the findings of the evaluation of the applicable CPS for conformance to the associated CP, including details of any discrepancies found? This is the second-most frequent area where audits fail. Most methodologies do not compare the requirements of the CPS to the CP. If the CPS omits requirements imposed by the CP, the FPKIPA would like to know about it. If a CPS is not 100% in accordance with the CP, the FPKIPA will want details on what's deficient.

Guidance	Commentary
Audit Includes Test Results State whether the auditor reviewed the PIV/PIV-I card test results (that are less than a year old).	If appropriate, did the PKI provide evidence of compliance with the FIPS 201 Evaluation Program Annual card testing? Did the PKI provide sample certificates of every covered issuing CA to the FPKI?
Audit Operational Findings State that the operations of all PKI components (Principal CA, other CAs, CSSs, CMSs, and RAs) were evaluated for conformance to the requirements of the applicable CPS. Report the findings of the evaluation of operational conformance to the applicable CPS.	Did each Audit Opinion Letter state whether the operations of the PKI components were evaluated for conformance to the requirements of the applicable CPS? Did each Audit Opinion Letter state the findings of the evaluation of operational conformance to the applicable CPS, including details of any discrepancies found? This is where most audits fail. As discussed in the guidance, a plain vanilla WebTrust for CA audit will not meet this requirement, as the suggested controls in the WebTrust methodology do not necessarily capture all of the CPS requirements. If the operations are not 100% in accordance with the CPS, the FPKIPA will want details on what's deficient.
Audit MOA Findings State that the operations of the PKI Owner/Operator's Principal CA and any other relevant components were evaluated for conformance to the requirements of all current cross-certification MOAs executed by the PKI with other organizations. Report the findings of the evaluation of the conformance to the requirements of all current cross-certification MOAs executed by the PKI Owner/Operator.	Did each applicable Audit Opinion Letter state that the relevant PKI components were evaluated for conformance to the requirements of all current cross-certification MOAs executed by the PKI with other organizations? Did each applicable Audit Opinion Letter state the findings of the evaluation of conformance with applicable MOAs, including details of any discrepancies found? In many instances, the MOA imposes requirements on CAs or other PKI components. These should be examined. If there is anything other than 100% compliance with MOA-imposed requirements, the FPKIPA would like to know about it. For MOAs with the FPKIPA, is the MOA consistent with the latest FPKI MOA Template?
Previous year findings Did the auditor review findings from previous year and ensure all findings were corrected as proposed during the previous audit?	Often, the auditor sees an Audit Correction Action Plan, POA&M, or other evidence that the organization has recognized audit findings and intends to correct them, but the auditor is not necessarily engaged to assess the corrections at the time they are applied. The auditor should review that all proposed corrections have addressed the previous year's findings.

Guidance	Commentary
Changes Because the FPKI relies on a mapped CP and/or CPS for comparable operations, has the auditor been apprised of changes both to documentation and operations from the previous audit?	CPs change over time and each Participating PKI in the FPKI has an obligation to remain in synch with the changing requirements of the applicable FPKI CP (either FBCA or COMMON Policy) – has the participating PKI's CP and CPS been updated appropriately? If there have been other major changes in operations, has a summary since the last year's audit been provided or discussed with the auditor?
Audit Signature Each audit opinion letter and audit review report is prepared and signed by the auditor.	Was each Audit Opinion Letter prepared and signed by the auditor? Yes, the report needs to be signed – wet signature or electronic. As a practical matter, it is good practice to include contact information for the auditor (e-mail and telephone number) in case further clarification is needed.
Sample certificates	Because the FPKI relies on sample certificates to ensure the PKI is compliant with profile requirements, interoperability, and reporting, sample certificates of all types issued within the last year must be submitted to the FPKIPA.
Test reports A test report from the FIPS 201 Evaluation Program was received for each PIV/PIV-I configuration issued	Were all required PIV or PIV-I card test reports provided?

Appendix D – Glossary

Bridge	A PKI Bridge enables interoperability between different PKIs by asserting comparability in certificate policies. In the context of the FPKI, a Bridge refers to the organization that operates a Bridge CA and represents a community of interest in a peer-to-peer relationship with the FPKI.
CA	Certification Authority Central component of a PKI. An authority trusted by one or more users to issue and manage X.509 Public Key Certificates and CRLs.
COMMON	The X.509 U.S. Federal Public Key Infrastructure Common Policy Framework Root Certification Authority The trust anchor of the Federal PKI.
CP	Certificate Policy The governing document of the PKI.
CPS	Certification Practice Statement Companion document to the CP. Describes how the requirements of the CP are implemented within the PKI operational environment.
CMS	Card Management System
CRL	Certificate Revocation List A list maintained by a Certification Authority of the certificates which it has issued that are revoked prior to their stated expiration date.
CSS	Certificate Status Server Provides on-line verification to a Relying Party of a subject certificate's trustworthiness.
FBCA	Federal Bridge Certification Authority Facilitates trust on behalf of the FPKI among distinct PKI domains through peer-to-peer cross-certification.
FPKI	Federal Public Key Infrastructure The entire trust fabric anchored in the Federal COMMON Policy Root and further facilitated by the Federal Bridge Certification Authority.
FPKIPA	Federal Public Key Infrastructure Policy Authority Governing body of FPKI. Operating under the auspices of the CIO Council.
FPKI SSP	Federal Public Key Infrastructure Shared Service Providers Organization operating a PKI in accordance with the requirements of the COMMON CP and subordinated under the COMMON CA for the purpose of issuing Personal Identity Verification credentials to Federal employees.
Management Assertion	A Management Assertion is a document signed by an authorized representative of the PKI to explicitly acknowledge that the PKI is operated in accordance with all of the requirements of the CP and MOAs and meets all security requirements.
MOA	Memorandum of Agreement
PIV	Personal Identity Verification Mandated by HSPD-12 and defined in NIST FIPS 201-2, this is the common standard identity credential for the executive branch of the Federal government.
PIV-I	Personal Identity Verification Interoperable Identity credentials issued in a manner that makes them technically interoperable with the Federal PIV credential, and containing digital certificates issued by a CA cross-certified with the FPKI at the PIV-I level of assurance.
PKI	Public Key Infrastructure
PKI Owner/Operator	Organization responsible for the policies, procedures and operations of the PKI

POA&M	Plan of Action and Milestones In the event there are Audit findings, the Plan of Action and Milestones is used to itemize the findings, identify the planned remediation and track the action to its completion.
RA	Registration Authority The entity responsible for the identity proofing and enrollment of end users within the PKI
Third-Party Auditor	An individual/company, separate and distinct from the PKI owner/operator, that conducts an independent review of the policies, procedures and operations of the PKI and renders an opinion concerning the PKI's compliance.